



JP63311455



COPY PROTECTION DEVICE FOR SOFTWARE

Patent Number: JP63311455
 Publication date: 1988-12-20
 Inventor(s): FUJINAMI YASUSHI
 Applicant(s):: SONY CORP
 Requested Patent: ☐ JP63311455
 Application: JP19870146241 19870613
 Priority Number(s):
 IPC Classification: G06F12/14 ; G06F9/06
 EC Classification:
 Equivalents: JP2569564B2

Abstract

PURPOSE: To secure copy protection even to remodeling by collating data on software simultaneously with the reading action of the software and fetching a copy protection code via a register to inhibit the output of said code to the outside.

CONSTITUTION: A decoder 24 is connected to an address bus 23 and outputs H as a selection signal when an address reaches another address where copy protection data is written. A gate circuit 25 receives a selection signal from the decoder 24 and switches a control bus 21. Then a selection signal SEL of H is supplied to the circuit 25 from the decoder 24 with a copy protection code when a floppy disk FD40 is read. At the same time, a chip-enable signal of the bus 21 is supplied to a register 11 and the copy protection code is written in the register 11. In this case, nothing is written in a cache RAM41. Thus a copying action is impossible for the floppy disk even with remodeling.

Data supplied from the esp@cenet database - I2

(19) 日本国特許庁 (JP)

(12) 特 許 公 報 (B2)

(11) 特許番号

第2569564号

(45) 発行日 平成9年(1997)1月8日

(24) 登録日 平成8年(1996)10月24日

(51) Int.Cl.	識別記号	庁内整理番号	FI	技術表示箇所
G06F 12/14	320		G06F 12/14	320E
9/06	550		9/06	550Y

発明の数1(全 6 頁)

(21) 出願番号	特願昭62-148241	(73) 特許権者	999999999 ソニー株式会社 東京都品川区北品川6丁目7番35号
(22) 出願日	昭和62年(1987)6月13日	(72) 発明者	藤波 靖 東京都品川区北品川6丁目7番35号 ソ ニー株式会社内
(85) 公開番号	特開昭63-311455	審査官	野仲 松男
(43) 公開日	昭和63年(1988)12月20日	(56) 参考文献	特開 昭61-195427 (JP, A) 特開 昭69-231650 (JP, A)

(54) 【発明の名称】 ソフトウェアのコピープロテクト装置

1

(57) 【特許請求の範囲】

【請求項1】 ソフトウェアが書き込まれた記録媒体を読出すと共に、ソフトウェアの書き込みを行う装置であって、

データの書き込み・読出しを制御するための、1チップ化されたコントロール回路と、

このコントロール回路内に設けられたレジスタと、

このコントロール回路により記録媒体に書き込み・読出し動作を行う記録・再生回路とよりなり、

ソフトウェアの読出し動作と同時にそのソフトウェアのデータを照合し、通常のデータに関しては外部に出力可能とし、コピープロテクトコードに関しては上記レジスタに取り込むことで外部からの書き換えを不可能にしたことを特徴とする、ソフトウェアのコピープロテクト装置。

2

【発明の詳細な説明】

【産業上の利用分野】

本発明は記録媒体上のソフトウェアを読出し、他の記録媒体にコピーを行うことを制限する装置に関するものである。

詳しくは、フロッピーディスクの如き記録媒体からソフトウェアを読み出して実行させる如きコンピュータ装置に関し、読出したソフトウェアを他のフロッピーディスクに無制限にコピーすることを防止するフロッピーディスクのコピー・プロテクト装置に関する。

【従来技術】

ソフトウェアのコピーを防止する装置として、特開昭59-357747号などが公知となっている。このような技術では、一般にフロッピーディスク上に本来のソフトウェアデータと、コピープロテクトデータとが混在して記録さ

(2)

特許2569564

3

れており、コピープロテクトデータによりコンピュータ装置が自己判断してコピーを禁止する動作を行う。このような装置をさらに図面を参照しながら、詳細に説明をする。

第3図は本願に係るコンピュータ装置30の構成を示す。コンピュータ装置30はプロセッサ31（以下CPUと称する）とメインRAM32がバス33を介して接続されており、さらにフロッピーディスクドライブ装置35（以下FDDと称する）を内蔵する。このFDD35は内部にIC化された、フロッピーディスクコントローラ36（以下FDC）を有する。FDC36は、内部にコントローラ37と記録・再生回路38とを持つ。記録・再生回路38は磁気ヘッド39によりフロッピーディスク40（以下FDと称する）上のデータの読み出し・書き込みを行う。更にFDC35には比較的大容量のキヤツシユRAM41が接続されている。このキヤツシユRAM41はCPU31からのアクセスに対して、キヤツシユレジスタとしての効果と、バッファレジスタとしての効果をもつ。

さて、FD40上には、第4図に示すフォーマットのデータが書き込まれている。尚、説明を簡略化する為、本願に直接関係のないデータについては、斜線で示し、説明を割愛した。aは1トラックのデータフォーマットを示す。1トラックは4つのセクターS（1）～S（4）で構成され、各セクターは5765B（バイト）のデータに決められている。bは各セクターの内部構造を示し、内部に0番から127番のデータフレームDF（0）～DF（127）まで128個のデータフレームに分割されている。各データフレームは44Bの容量に決められている。さらにcに示すように、各データフレームは1Bのサブコード（SC）と32Bのコーディングデータ（CD）及び誤り訂正のための8Bのバリテイデータ（PD）に分割されている。各データフレームに1Bのサブコードが存在し、全データフレームでは128Bのサブコードが存在することになる。これらのサブコードはdに示すように4組の同じものよりなり、各32Bに2Bのコピープロテクトコード（CPU）が存在する。

さて、FDC36はFD40の各種データから、誤り訂正されたデータとコピープロテクトコードとを外部に出力可能とする。通常、これらのデータはキヤツシユRAM41に蓄積され、CPU31からの要求により、データだけをメインRAM32に転送する。

コピープロテクトコードの使用方法は、以下第5図～第7図を参照しながら説明する。

まず、第5図において、50・51は夫々メインRAM32・キヤツシユRAM41のメモリマップを概略で示したものである。CPU31はキヤツシユ41のコピープロテクトコード（〇〇〇）を読み、CPU31自身が持つコピープロテクトコード（〇〇〇）と比較する。このCPUの持つコピープロテクトコードは、ROM52としてCPU31に組み込まれている。読み出されたデータがオリジナルのFDのものであれ

4

ば、コピープロテクトコード（〇〇〇）は一致し、メインRAM32に転送されているソフトウェアにより、正常に実行する。

さて、他のFD（X）にメインRAM32のソフトウェアをコピーする場合、コントローラ37はコピープロテクトコードとして本来の（〇〇〇）に換えて、ROM52内のダミーのコード、例えば（×××）を書き込むように動作する。こうしてコピーされたFD（X）のソフトウェアは、コピープロテクトコードだけが（×××）となったソフトウェアとなる（第6図）。

このコピーのFD（X）を読み出して動作させようとする時、キヤツシユRAM41のコピープロテクトコードは（×××）であり、CPU31の持つコピープロテクトコード（〇〇〇）と異なることになる。そこでCPU31はFD（X）が違法にコピーされたものであることを検知し、正常な動作を禁止することができる（第7図）。

さて、以上の構成によれば、FD（X）は通常の行為では動作させることができないが、次のような改造により、動作させることが可能であることがわかった。即ち、予めオリジナルのFDを読み出した時、キヤツシユRAM41に書き込まれたコピープロテクトコード（〇〇〇）を知っておく。次にコピーのFD（X）からデータを読み出した時、キヤツシユRAM41上のコピープロテクトコード（×××）を外側からの操作により、（〇〇〇）に書き換えてしまうのである。こうすると、FD（X）がコピーであるのにもかかわらず、CPU31からコピープロテクトコードをアクセスすると、（〇〇〇）が存在するので、メインRAM32のソフトウェアは実行可能となってしまう。FDC36に対して、キヤツシユRAM41は外付けされているので、この間のバス34にメモリの内容を書き換える治具を挿入するなどして、部分書き換えを行うことは、高度の電子技術を持つ者には比較的容易に可能である。このような改造行為は、明らかに著作権法に違反し、処罰の対象となるが、未然に防止できることが好ましい。

〔発明の目的〕

本発明の目的は、前述のような改造に対してもコピープロテクトを可能とすることを目的とし、具体的にはコピープロテクトコードを外付けのキヤツシユRAMに出力しないようにすることにある。さらに具体的にいえば、1チップ化したFDC内部に比較的小容量のレジスタを設け、通常のデータは外部のRAMに出力可能とするとともに、コピープロテクトコードに関しては、外部に出力することを禁止し、FDC内のレジスタに書き込むことを特徴とする。

〔発明の実施例〕

以下、この発明の実施例を添付図面に即して詳細に説明する。

第1図は本発明によるFDCの構成を示す。従来と同じものについては、第3図の説明で使用した番号をそのまま使用している。本発明の特徴は、1チップのICであるFDC1

(3)

特許2569584

5

6

α内に、レジスタ11を設けた点にある。このレジスタ11はコピープロテクトデータが一時記憶できる程度の比較的小容量で良い。本発明の実施例では、28で構成した。コントローラ37はデータ列又はアドレスを検知しており、コピープロテクトコード部になると、キヤツシユRAM41へのデータ出力を禁止し、レジスタ11への書き込み動作を行う。キヤツシユRAM41からメインRAM32へのデータ転送は通常のように行われる。実行に際しては、CPU31がコピープロテクトコードを要求すると、コントローラ37はレジスタ11のコピープロテクトコードを返す。以上のように、オリジナルのFDであれば、従来と動作上異なることはない。

コピーのFD(X)を読み出した場合、キヤツシユRAM41にはデータが、レジスタ11にはコピープロテクトコード(×××)が書き込まれる。このコピープロテクトコード(×××)は1チップ化されたFDC10にあるので、外部から書き換え操作を行うことは不可能である。CPU31とFDD35との間のバス33を介して、コピープロテクトデータが盗まれる可能性はあるが、レジスタ11のコピープロテクトコードを書き換えることができないので、コピーのFD(X)を実行することは不可能である。第2図は上述の実施例をさらに具体構成で示したものである。FDC10内にはコントロールバス21、データバス22及びアドレスバス23がある。各バスは、夫々以下に述べる各デバイスに接続されている。記録・再生回路38、及びコントローラ37については既に述べたので説明を割愛する。レジスタ11は各バスに接続され、キヤツシユRAM41と並列の関係に設けられている。デコーダ24はアドレスバス23に接続され、アドレスがコピープロテクトデータの書き込まれているアドレスに至ると、選択信号として「H」を出力する。ゲート回路25はデコーダ24の選択信

*号を受けてコントロールバス21に切り換える。コントロールバス21は、例えばキヤツシユRAM41及びレジスタ11のチップイネーブル端子(CE)に接続されているので、キヤツシユRAM41又はレジスタ11を択一動作させる。FD40の読出し動作において、通常のデータ列ではゲート回路25がキヤツシユRAM41を選択している。データがキヤツシユRAM41上に書き込まれる。所定のアドレスに至り、コピープロテクトコードとなると、デコーダ24より「H」の選択信号(SEL)がゲート回路25に供給され、ゲート回路25はコントロールバス21のチップイネーブル信号をレジスタ11に供給し、コピープロテクトコードはレジスタ11に書き込まれる。この時、キヤツシユRAM41には何も書き込まれない。

この実施例では、コピープロテクトコードのアドレスが決まっていることを前提に、デコーダ24の入力をアドレスバス23に接続した。他の方法としては、データを常に監視する回路をデータバス22に接続し、データバスにコピープロテクトコードの開始を表すコードの存在を検知したら、ゲート回路25に選択信号(SEL)を供給してもよい。

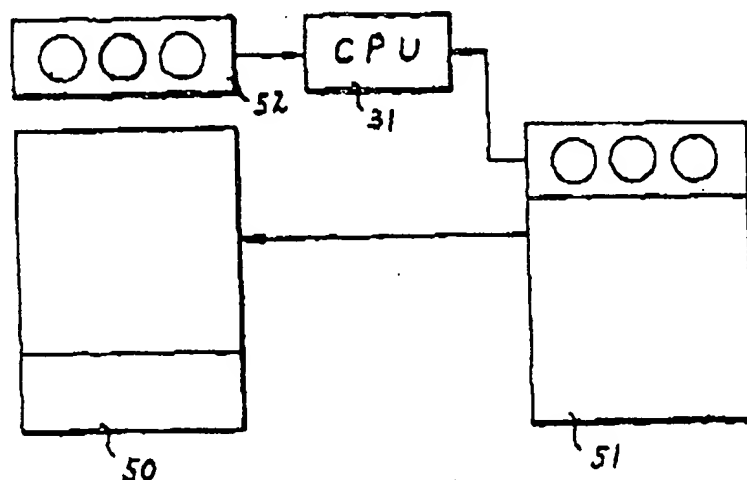
【発明の効果】

以上説明したように、本発明のコピープロテクト装置によれば、改造によってもフロッピーディスクのコピーが不可能となる。

【図面の簡単な説明】

第1図は本発明のコピープロテクト装置の概念を示すブロック図、第2図は本発明の実施例を詳細に示したブロック図、第3図は従来のコピープロテクト装置のブロック図、第4図は本発明に係るフロッピーディスク上のデータフォーマットの概念図、第5図～第7図は本発明を理解するためのメモリマップを示す。

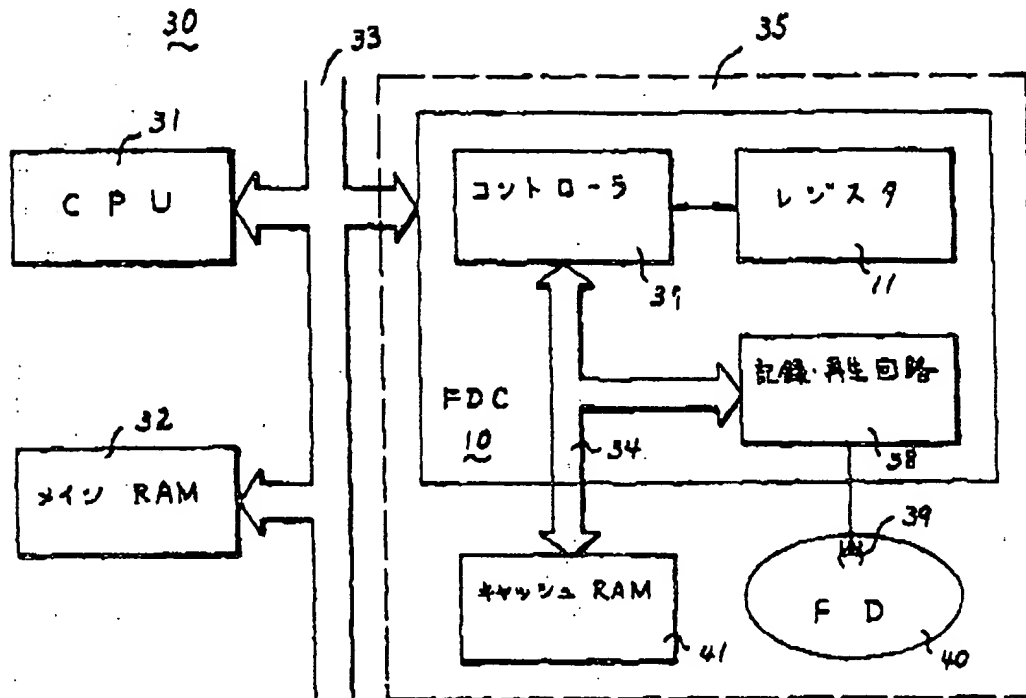
【第5図】



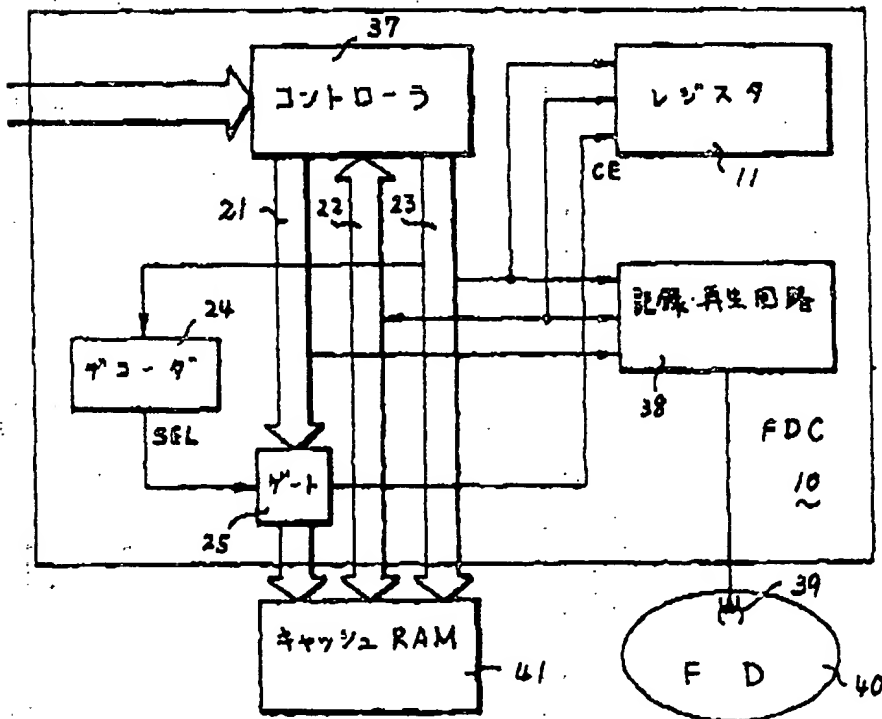
(4)

特許2569564

【第1図】



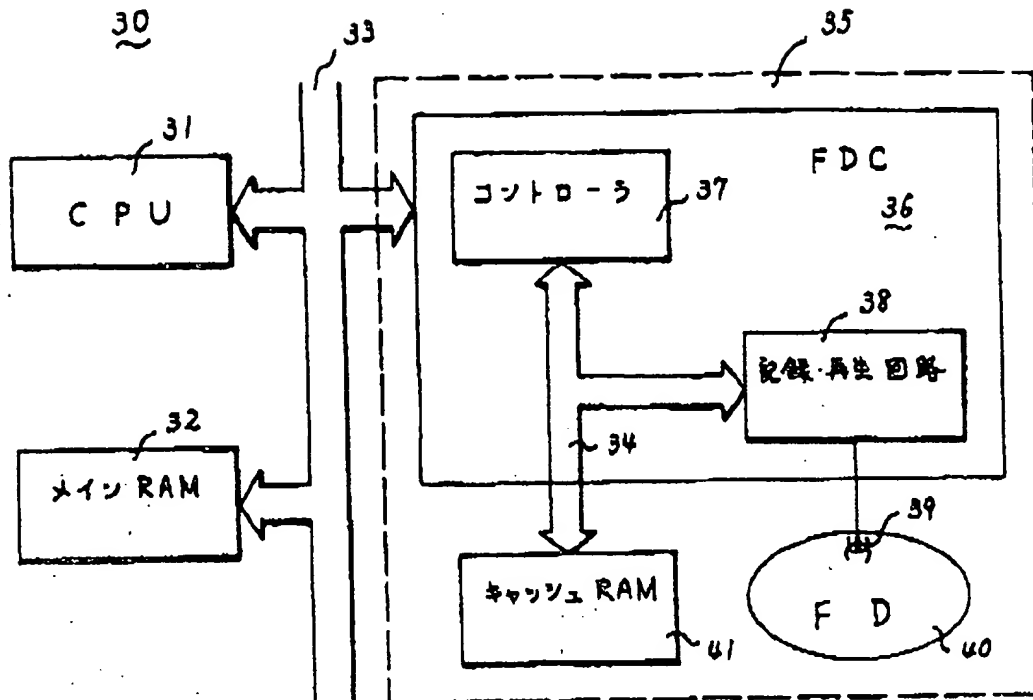
【第2図】



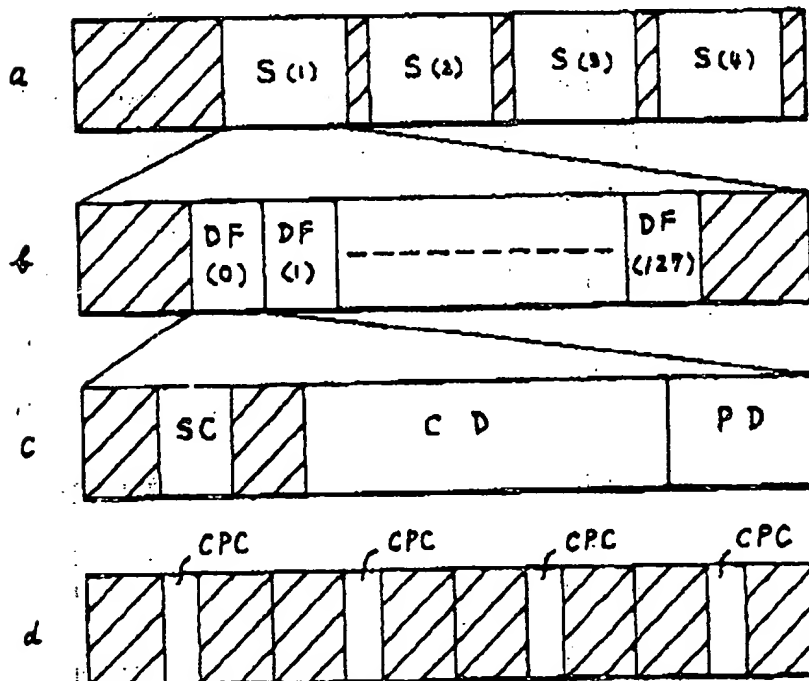
(5)

特許2589564

【第3図】



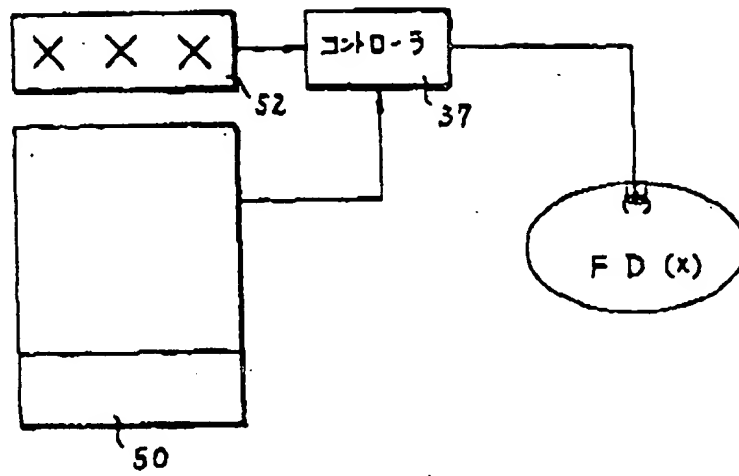
【第4図】



(6)

特許2589584

【第8図】



【第7図】

